PLEASE CIRCULATE QUICKLY AND INDICATE WHETHER A COPY IS REQUIRED FOR RETENTION — Y.37

Interrogation Report on POW TEMP Enrique

~~N.S.S.~~ ENS ✓
I.S.O. ~~H.H.A.~~ VA
~~Mr. Coleman~~ MNS
~~N.S.I.~~
~~N.S.II.~~
~~N.S.III.~~
~~N.S.IV.~~
N.S.V.
~~N.S.VI.~~
~~N.S.VII.~~
~~I.S.S.~~ (I) ~~MINTS~~ ~~CAPTS~~ ✓

Disposal D of R for Cal Manson

No 82

Date 26/7/45

DS/1348

Y.37

PLEASE [illegible] AND INDICATE

WHETHER A [illegible] REQUIRED [illegible]

Copy No: 14

D.D.4
Major Morgan. 1 copy please GWM.
D.D.(N.S.) 1 copy please [illegible]
~~Comdr. Mahoney U.S.N.~~ 1 copy [illegible]
S.A.C.

Copy No: 17

D.D.(C.S.A.)
Commander Tighe, D.S.D.10. Copy [illegible]
Admiralty.
D.S.D.4.X. Copy Sent
S.A.C.

Attached is a copy of a interrogation report on Pow Enrique TEMP who worked at OKM 4 SKL III, 1943 - 1944, thereafter serving with the B Groups NERVI and SAN REMO as assistant cryptographer and translator.

Items of particular interest are :

Pages 9 - 19. Details of cryptanalytic work on British Naval Code (München) (Braun - Auxiliary Vessels).

"Traffic became unreadable on 1st January 1944 and continued to be so" - page 10.

Page 20.

(a) Naval Cipher No: 3 (Frankfurt). - No success after February 1943.

(b) LOXO and COFOX. - Traffic read until the end.

Margaret Oliver for
R Dudley-Smith

S A C.

~~TOP SECRET~~

CSDIC/CMF/ Y37

Copy No:

FIRST DETAILED INTERROGATION REPORT ON

TEMP Enrique.

Name	:	TEMP Enrique.
Rank	:	Matrose (Civilian in equivalent rank).
Unit	:	"B" GRUPPE SAN REMO (German Navy).
Function	:	Asst cryptographer & translator, later WT Mechanic.
F.P. No.	:	02516 (?)
Captured	:	10 May 45, GENOA.
Secret No	:	M45/611
Interrogated	:	CSDIC/CMF 1 - 12 Jun 45.

I N D E X

Page

1. PREAMBLE 2

2. HISTORY AND MOVEMENTS 2

3. ORGANISATION OF GERMAN NAVY INTERCEPT SERVICE ("B" - DIENST) 3

A. OKM SKL 3
B. Chef MND 3
C. 4 SKL III 3

I. Cryptographic Service 3
(a) The "General Referate" 3
(b) The "Referate" 3
(c) The Secs &/or Groups 4
(d) Personnel 4

II. Intercept and DF Service 5
(a) The Naval DF HQs (MP Abt) 5
(b) The Naval Main DF Stns (MPHS) 6
(c) The Naval DF Sub-Stns (MPNS) 6
(d) The "B" Gruppen 6

4. LOCATIONS (A - G) 7

5. EQUIPMENT (A - C) 8

6. WORK AT Fu REFERAT (MUENCHEN BRAUN) - THE AUXILIARY VESSELS CODE 9

A. History 9
B. Description of Code and Recipher System 10

I. The Code Book 10
II. The Recipher System 11
III. Traffic and Indicators 11

C. Cryptography - Methods and Results 12
I. Sorting of traffic 12
II. Breaking the Recipher, Methods used 12
III. Breaking the Recipher, Details 13
(a) Pairs of indicators 13
(b) "Suspected" subtractor group 13
(c) Chance repeats 14
(d) "Rolling" 15
(e) Deciphering of indicator groups 16
(i) "Chain of indicators" 16
(ii) "Ring of indicators" 16

INDEX (continued).

Page

(f) Differencing..... 17
(i) " as an aid to reciphor & code breaking..... 17
(ii) " for the purpose of finding pairs ("Serien")..... 18

IV. Registration of Code Groups..... 19

7. WORK AT Fu REFERAT (FRANKFURT) & OTHER SECS..... 20

A. The FRANKFURT System..... 20
B. RN and US Navy Tactical Codes..... 20

8. THE U-BOAT DF SERVICE..... 21

9. WORK AT GRUPPEN NERVI AND SAN REMO..... 21

10. PERSONALITIES..... 21

Appendix "A"- Pattern of German Navy Intercept WT Form..... 23
" "B"- " " " " " Log Book Form..... 24
" "C"- Details of WT Stns covered by German Navy Intercept Service, Call signs & Frequencies memorised by PW..... 25
" "D"- Description and use of "Rollmaschine" (w. sketch)..... 29
" "E"- PW's description of U-BOAT Special DF apparatus and exploits of a DF Operator (in German and English translation) 31

1. PREAMBLE

PW is a fairly bright young man of 26 of mixed German and Spanish origin. He claims to be a Spanish subject. His story is an unusual one, and his manner does not inspire confidence; at the same time there seems to be no obvious reason why he should want to mislead, unless he hopes to be repatriated to SPAIN, thereby avoiding internment. He talks freely, almost too willingly. Technical information is believed to be fairly sound, in spite of the fact that PW is not a cryptographer. PW speaks English, German, Spanish, French and a little Italian.

Reliability: Fair. (Interrogated by A.G.B.).

2. HISTORY AND MOVEMENTS

29 Aug 1918	:	Born in BARCELONA as the son (posthumously) of a Spanish father, Guillermo TEMP, and of a German mother Maria nee KUNZ. His mother remarried, in 1927, a German teacher, SCHAEFFER, who owned a private school in BARCELONA. (SCHAEFFER, born in 1900, served as a naval cadet in the first World War and joined the German Navy again during the present war. He comes of naval stock, one of his uncles being an admiral).
1933 - 38	:	Visited German High School at CALLE MOYA 4, BARCELONA.
Jul - Aug 39	:	Went to BERLIN to learn pharmacy. Apprenticed to Messrs BIEDELE HAHN.
Summer 41	:	Started work at Reichsvereinigung Chemische FASERN.
Mar 43	:	Called up to German Navy, and on account of his knowledge of English, posted to Cryptographic Service. (OKM SKL CHEF MND III).
Apr 43	:	Started work after a fortnight's course.
Dec 44	:	Transferred for reasons of health to ITALY, and posted first to "B" Gruppe NERVI, later to "B" Gruppe SAN REMO.
23 Apr 45	:	"B Gruppe" SAN REMO left for GENOA, but was stopped by a Partisan road block at COGOLETO. PW intervened and organized the bloodless surrender of the group, consisting of an offr and 40 ORs. Remained with Partisans.
10 May 45	:	Reported to British Naval Officer at GENOA, and taken into custody two days later.

3. ORGANISATION OF GERMAN NAVY INTERCEPT SERVICE ("B" DIENST).

A. GERMAN NAVY HIGH COMMAND- NAVAL WAR DIRECTORATES. (OBERKOMMANDO DER MARINE- SEEKRIEGLEITUNGEN - hereafter referred to as OKM SKL.).

PW knew of the existence of four Naval War Directorates (SEEKRIEG-LEITUNGEN = SKL) numbered 1 to 4, which he described as the "tactical commands" of the German Navy High Command (OKM). SKL 4 - known as 4. SKL after 1 May 44 - controlled the four HQs or bureaux dealing with the Naval Sigs Service (MARINE NACHRICHTEN DIENST = MND) - see B. below.

B. HQs NAVAL SIGS SERVICE (CHEF MARINE NACHRICHTEN DIENST = Chef MND).

Until 1 May 44 there were four HQs of the German Naval Sigs Service u/c SKL 4. These were called Chef MND I - IV, their full address always being preceded by reference to High Command and Directorate, for instance OKM SKL Chef MND IV.

Chef MND I &) dealt with German Navy Signals System and own codes
" " II) and ciphers.

Chef MND III dealt with Intercept incl. DF and Cryptography ("FUNK AUFKLÄRUNG" or "BEOBACHTUNGSDIENST" = "B" DIENST and ENTZIFFERUNG = EZ).

Chef MND IV dealt with Radiolocation and Defence against Radiolocation ("FUNK MESS" i.e. "ORTUNGSWESEN und ASDIC ABWEHR usw").

After 1 May 44 these HQs were known as 4 SKL I - IV, all under 4. SKL.

C. 4 SKL III (Formerly OKM SKL CHEF MND III)

This HQ, till 1 May 44 Chef MND III, when its organisation was the same, is best described under its respective functions of Cryptography, and Intercept and DF. It may be assumed that on the advice of the Referate dealing with cryptography the HQ controlled the intercept and cryptographic work (low-grade only) carried out by the Naval DF and Intercept units. It is not certain whether the HQ also controlled Admin and technical matters in these units.

I. Cryptographic Service (BERLIN)

PW does not know how the Evaluation Dept (AUSWERTUNG) fitted into the organisation. For purposes of cryptography work was organised into two "General Referate" and a number of "Referate", Seas and Groups.

(a) The "General Referate"

These were two in number, one called General Referat "F" dealing with ROYAL NAVY traffic and RUSSIAN NAVY, and the other General Referat "?" on "AMERIKA Abteilung", dealing with US NAVY. As PW joined the organization in Mar 43 he did not know how work was subdivided among Referate - general and ordinary - in the days when the French, Italian, Jugoslav and Greek navies etc had to be watched on the air. PW only knew the organisation of General Referat "F". This was sub-divided in several Referate and smaller seas or groups, according to countries, type of traffic, tasks and geographical subdivision of enemy wireless networks. See (b) and (c) below.

(b) The Referate of General Referat "F"

There were some five Referate in all, which had both a name and a cover-name.

~~TOP SECRET~~

CSDIC/CMF/Y 37

Referat	Cover name	Function
Fu Referat	FRANKFURT	Worked on High Grade R.N. codes.
Fn Referat	MUENCHEN BRAUN	Worked on R.N. Auxiliary Vessels code in use in HOME WATERS and ATLANTIC as far South as FREETOWN (recipher changing twice monthly).
	MUENCHEN BLAU	Worked on R.N. Auxiliary Vessels code in use in MEDITERRANEAN and INDIAN OCEAN (recipher changing three times a month).
? Referat	KOELN	No details known.
? Referat	GALLIEN	Worked on Russian Naval traffic.
Fm Referat (after Dec 43)	?	Work included that on Naval Attachés' traffic (see further (c) below).

One Referat dealt with SWEDISH Naval traffic.

(c) The Secs and/or Groups of General Referat "F"

These were smaller nuclei in General Referat "F" formed either ad-hoc and disbanded when work was ended, or permanent sub-divisions of General Referat "F" whose functions were not large enough to warrant the formation of a Referat. (NOTE: for the purpose of this report a Sec will be the name given to the former type of nucleus, and a Group that given to the latter type). The groups were either run as separate nuclei of 4 SKL III, or worked as specialised subordinate units of various Referate. PW remembered:-

Secs:

STETTIN - formed after the sinking of the BISMARCK, and only existed for about a fortnight.

HAMBURG - no details known.

BREMEN - Worked from about 42 to 44, on Naval Attache's traffic.

Groups

FRITZ OTTO (Fo) : formed about end 43. Worked for Fn Referat (MUENCHEN BRAUN) on differencing.

FRITZ MAX (Fm) : formed before 43. In Dec 43 took over the STETTIN, HAMBURG and BREMEN Secs, and became Fm Referat.

FRITZ Quatsch (Fq) : dealt with Crypto work at the Naval Main DF Stns (see II. b. below). Worked on tactical codes such as "LOXO".

"K" Gruppe : worked for Fu Referat. No details known.

"ROLL" Gruppe : dealt with "rolling" for all Referate and Secs and/or Groups working on recipher breaking.

NOTE: The HOLLERITH Abteilung which may or may not have been part of the orgn was available for special work.

(d) Personnel

A staff of about 700 to 800 civilians and Naval (incl Army and G.A.F transferred to Navy) personnel, male and female, worked at the HQ and in Crypto and Evaluation. Training was given to ALL personnel in offices by means of a 14 days course explaining generally the type, purpose and methods of the work.

Cryptographers attended the same special course which also lasted two weeks. PW stated that after 43 the OKM was constantly short of English speaking personnel. He also stated that he had been offered facilities to become an expert in cryptography, but that he had declined it. ("I felt that through my work I might do harm to a nation whose enemy I - a Spaniard(!) - am NOT"). CAs only got special trg by working - unofficially - under an i/c watch (WACHLEITER) and trying to improve their knowledge. NO special course was held as in OKH.

The staff worked in shifts called watches (WACHEN) under an i/c watch, (WACHLEITER) usually a PO specialised CA. Each watch consisted of approx 10 people: 1 - 2 CAs and 8 statisticians and translators. Rotation of watches proceeded as follows:

on 3 days from 0800 to 1600 hrs.
" " " " 1600 " 2300 "
" " " " 2300 " 0800 "
one day off duty
two days of "extra watch" (PLUSWACHE) from 0900 to 1500 hrs,
then as from the beginning again.

Security regs were strict. The official secrets act or regs were read out to personnel every month.

Office equipment was scarce, economy being the motto. Clerks had to buy their own india rubbers outside and even getting a pencil was a task of some difficulty.

II. Naval DF and Intercept Service

There were three types of station set up for DF and Intercept, known generically as "B" - STELLEN, or , from a cryptographic point of view, AUSSENSTELLEN. Though the main work of most of the stations consisted of intercept of WT and RT traffic, they were all referred to as DF (PEIL) Stations, i.e. Naval DF HQs (MARINE PEIL ABTEILUNGEN = M P Abt), Naval Main DF Stations (MARINE PEIL HAUPT-STELLEN = MPHS), and Naval DF Sub-stations (MARINE PEIL NEBENSTELLEN = MPNS). There were also small dets called "B" - GRUPPEN.

Traffic intercepted of ROYAL NAVY, US NAVY, RUSSIAN & SWEDISH NAVIES , was sent in part by TP to 4 SKL III. Approx 2,000 messages a day were received in BERLIN from the Aussenstellen. (Details sent by TP were the heading or preamble, and the first five and last five groups of all messages).

(a) Naval DF HQs (MP Abt)

These were the largest fixed stas. According to PW there were two in existence, one (MP Abt DEUTSCHE BUCHT) at WILHELMSHAVEN/SENGWAARDEN, the other (MP Abt FLANDERN) at BRUGES (till mid-summer 44). They appear to have been formed during the war (FLANDERN for certain) or in any case raised to the status of HQs (ABTEILUNGEN). They came directly under 4 SKL III for operational control at least.

Their work was mainly intercept. CAs were attached for dealing with low grade traffic. In addition MP Abt FLANDERN trained, equipped and posted U-Boat DF and RT Intercept operators (see para 8 and App "E").

Both MP Abteilungen controlled a number of Naval DF Sub-stations (MPNS). See under (c) below.

Each MP Abt had the following personnel:-

approx 25 sets (zones = BEREICHE) with 100 WT operators.
" 20 statisticians/clerks
" 10 cryptographers
" 10 orderly room and LT personnel
" 30 guard personnel

~~TOP SECRET~~

CSDIC/CMF/Y 37

(b) Naval Main DF Stations (MPHS)

There was a substantial number of these, some of which had been in existence since before the war, viz. MPHS AHLBECK, LANGENARGEN and SOEST. For other locations see para 4.

They dealt mainly with Intercept, and came under 4 SKL III for operational control at least. They themselves controlled the work of the small dets ("B" - GRUPPEN), and of some of the MPNS.

Personnel of each MPHS was as follows:-

approx 15 sets (zones=BEREICHE) with 60 WT operators.
" 10 statisticians/clerks.
" 5 cryptographers.
" 5 orderly room and LT personnel.
" 20 guard personnel.

(c) Naval DF Sub-stations (MPNS)

These, (for Locations see para 4) concentrated chiefly on DF, though some Intercept work was done. They confined themselves to lower grade traffic. They came under either an MP Abt or an MPHS. Thus, all MPNS in NORWAY and the BALTIC area as far West as BORKUM were under MP Abt DEUTSCHE BUCHT, those in HOLLAND, BELGIUM and NORTH FRANCE under MP Abt FLANDERN.

They formed a network called the "DF-network" (PEILNETZ), which however did NOT cooperate with the other services (AA, GAF etc), for matters relating to AA defence, Coastal defence, bombing of convoys, etc. Stas used GAF LT for the purpose of intercomm. E.g. if "ANSATZ Quatsch" was called over the telephone, this meant that a bearing had been obtained on a unit signalling in WT on 124.5 m (For RT the call was "ANSATZ Quatsch - Fonie"). (Convoy escorts frequency, see also Appendix "C" para C.). The matter was reported to MP Abt FLANDERN and cuts and locations obtained reported to BERLIN. PW did not know how results were evaluated (? U-boats etc.).

Each MPNS had as personnel:-

approx 5 sets (zones=BEREICHE) with 20 WT operators.
4 DF operators
2 orderly room and LT personnel.
Guards supplied by other Navy units.

(d) "B" - Gruppen

These were small intercept groups or dets placed in points of tactical importance. Sometimes in addition to being u/c of an MPHS they were at the same time u/c of a local formation as well, e.g. "B" Gruppe NERVI was u/c 7 Security Div, but also under MPHS KARERSEE.

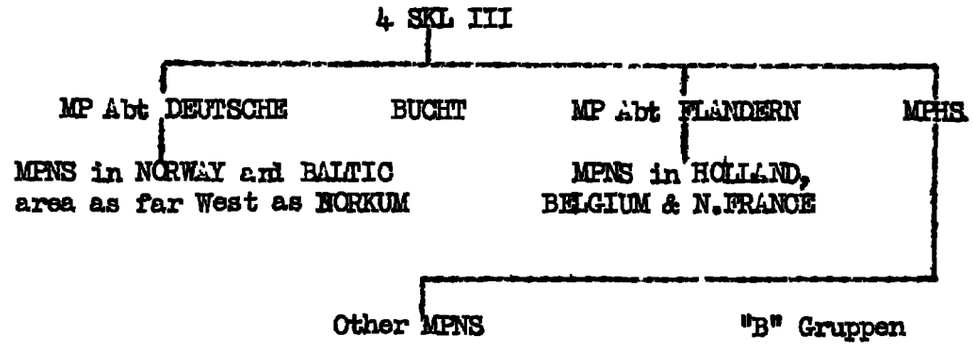
In ITALY at various times there were "B" Gruppen at ROME, VENICE, TRIESTE, NERVI, SAN REMO and PADUA.

Personnel varied from Group to Group. Thus NERVI had 1 officer, 2 Funkmeister, 6 NCOs, and 6 men, whereas SAN REMO had 1 officer and 40 ORs.

For details of work of "B" - Gruppen NERVI and SAN REMO see para 9.

NOTE: The following diagram illustrates the operational chain of command for the DF and Intercept service:-

(see over)



4. LOCATIONS

NOTE: (Inf contained in sub-paras C - G should be taken with some reserve).

A. OKM SKL Chef MND III (Renamed 1 May 44 - 4 SKL III)	: from beg war to 22/23 Nov 43)	In OKM bldgs 72-76, TIRPITZ UFER, BERLIN, W.35., except General Referat "?" (Amerika Abteilung) in the KUNSTSEIDE HAUS, 4, MESSDAMM, BERLIN-CHARLOTTENBURG.
	: from end Nov 43 to Feb/Mar 45)	With OKM, in Pz GREN KASERNE, EBERSWALDE nr BERLIN.
	: after Feb/Mar 45	ZURICH, between BERLIN & [illegible]SLAVEN (later ?)
HOLLERITH (?) Abteilung	: from 39 to Feb 44)	Under NIKOLAI KIRCHE, BERLIN-[illegible]ERSDORF.
	: after Feb 44)	EBERSWALDE.

B. Naval DF HQs (MARINE PEIL ABTEILUNGEN)

MP Abt DEUTSCHE BUCHT		: WILHELMSHAVEN/SENGWARDEN.
MP Abt FLANDERN	: till mid Jun 44	: BRUGES (TERLINDEN).
	: after bombing	: Split into an MPHS and an MPNS, both at BRUSSELS.

C. Naval Main DF Stations (MARINE PEIL HAUPTSTELLEN).

MPHS BRUSSELS	: Outside BRUSSELS in or near Kings Castle.
MPHS AHLBECK	: Near SWINEMUENDE; in existence before 1939.
MPHS BEELITZ	: Nr BERLIN.
MPHS LANGENARGEN	: On Lake CONSTANCE. Existed before 1939.
MPHS SOEST	: In RHINELAND nr COLOGNE. Most important sta; existed before 1939. Took US Navy traffic.
MPHS GRONINGEN	: No details known
MPHS KIRKENESS	: Formed in NORWAY in '40.
MPHS STAVANGER	: Formed in NORWAY in '40.
MPHS HJOERING	: Formed in N.DENMARK in '40.

MPHS BREST (Stas at LORIENT & BAYEUX) (?)	: No details known	
MPHS MONTPELLIER	: " " "	Possibly not all were MPHSs
MPHS BORDEAUX	: " " "	
MPHS KARERSEE (LAGO di CALDARO)	: Nr BOLZANO. Formed in mid 44, intended to be Emergency HQ (AUSWEICHSTELLE) for OKM, then at EBERSWALDE.	
MPHS (?) ATHENS MPHS (?) ROME	: PW was not sure of these and could not supply any details.	

D. Naval DF Sub-Stations (MARINE PEIL NEBENSTELLEN).

MPNS BRUSSELS	: LONGCHAMPS, in bldg nr the Belgian Tennis Club. U/c MP Abt FLANDERN.
MPNS BORKUM	: U/c MP Abt DEUTSCHE BUCHT. Did intercept work as well as DF.
MPNS DEN HELDER	: Cover name HELENE. After 6 Jun 44 also did intercept work. U/c MP Abt FLANDERN.
MPNS MAASLOUIS	: Cover name MAUSI. U/c MP Abt FLANDERN.
MPNSs (two stas) BRUGES	: Cover names: BRIGITTE (DF on 100-200 m wave band (GRENZWELLEN)), and BLANCA (DF on short wave traffic only). U/c MP Abt FLANDERN.
MPNS CAP GRISNEZ	: Bombed out in May 44, moved to ETRETAT. Did Intercept work as well as DF. U/c MP Abt FLANDERN.
(?) MPNS TORMIN	: Perhaps existed till 43 (?).

E. German Navy Sigs Experimental Commands (NACHRICHTEN VERSUCHS KOMMANDOS).

NVK - KIEL WIEK (HAGENUK)
NVK - PELZERHAKEN (nr LUEBECK).

F. German Navy Intercept and DF Stas in Spain.

These were known under cover names and had locations stated below:

MARK CASA	at	MADRID
MARK RASEN	"	SEVILLA
MARK NORTE	"	VIGO

G. "B" Gruppen IN ITALY (dates not certain).

ROME	
VENICE	
TRIESTE	
NERVI (under MPHS KARERSEE).	Still in existence Apr 45 (?)
SAN REMO (under MPHS KARERSEE).	Still in existence Apr 45.
PADUA (plus WT sta).	

5. EQUIPMENT

PW supplied details of RT and WT intercept and DF equipment used by some of the Intercept Stas working under 4 SKL III.

Type:	Makers:	Used At:
A. RT Intercept Sets:		
HRO (see + below)	National Company (sic) USA.	(MP Abt FLANDERN; FLANDERN (MPHS BRUSSELS and GRONINGEN.
CR 101	Philips	" " " "
DRCM	Societe Radio Francaise	" " " "
R34 RADIONE	Dr. Eltz - VIENNA.	" " " " and also "B" - Gruppen NERVI and SAN REMO.
SCHWABENLAND	Lorenz - BERLIN	MPHS GRONINGEN & KARERSEE.
SKYRIDER	USA firm, name not known to PW	MPHS HJOERRING.
SADIR UKW	Sadir (FRANCE)	MPHS GRONINGEN; MPNS ETRETAT & "B"- Gruppe SAN REMO.
Fu HED UKW	German made, firm not known to PW.	MPHS GRONINGEN.
B. WT Intercept Sets:		
HRO (see + below)	National Company (sic) USA.	MP Abt FLANDERN; MPHS GRONINGEN.
LO 6 K	Lorenz - BERLIN	MPHS GRONINGEN
LO 6 L	" "	" "
SCHWABENLAND	" "	" "
C. DF Sets (for WT and RT).		
E P 2	Telefunken	MP Abt FLANDERN; MPHS GRONINGEN: MPNS DEN HELDER.
ADCOCK CR 101	Philips	" " "

+ PW stated that HRO sets were known to exist in BELGIUM and that the German authorities made drives to requisition them. Soldiers, sailors etc were promised 14 days leave if they helped to unearth such sets. "These sets are THE best for intercept work" PW said.

6. WORK AT Fn REFERAT (MUENCHEN BRAUN).
The AUXILIARY VESSELS CODE.

A. History

(PW worked on this code from Mar 43 to Dec 44). It was the name by which the Germans referred to the code used by trawlers, etc, in comms with land bases, ports and other auxiliary vessels. PW could not say whether the RN referred to it by this name or not. The Germans had been working on this code since the war began. The Fn Referat (MUENCHEN BRAUN) dealt exclusively with traffic in this code covering HOME WATERS and ATLANTIC as far South as FREETOWN.

When PW joined the Fn REFERAT the current code-book had been in use for about nine months. The code was reciphered with the aid of subtractors tables or book (WURMBUCH) which changed fortnightly. (Code group subtracted from recipher group - PW quoted formula W-C=F i.e. WURMGRUPPE minus CODEGRUPPE=FUNKGRUPPE).

PW thought that this code book was the 3rd edition in use(?). It had been reconstructed to the extent of 60 to 70% with the aid of a previously current code

book captured on CRETE, or another island in the MEDITERRANEAN. The captured book had been photographed and issued in the form of a photostat copy to the Fu Referat. It bore the title "NAVAL CODE No 5". This made PW conclude that the book in use from approx Jul 42 to Apr 43 was called "N.V.L CODE No 6", but said he was not sure of this.

The (?) No 6 Code Book was changed at end Apr or beg of May 43, but the same recipher book continued to be used. From beg May 43 to about Jul 43 nothing was read until a cryptographer, Cadet (Faehnrich) LUSEBRINK (later Sub Lieut-Leutnant) noticed that analysis of May, Jun & Jul traffic revealed that FREETOWN had continued to use the (?) No 6 code book for 14 days after all other bases etc had changed over to the new book. This overlap allowed the German Navy cryptographers to break part of the new book.

In Dec 43 the recipher book was changed, the code book introduced in Apr/May 43 continuing to be in use. The recipher book or set of tables was now changed daily. The period of approx four weeks (? 1 Dec 43 to 1 Jan 44) was considered by PW as a transition period, for on 1 Jan 44 the traffic became unreadable and continued to be so till Dec 44, when PW left the OKM. (Watches were now - in 44 - only two per diem i.e. 0800 to 1200 hrs and 1200 to 2000 hrs). From friends' letters to PW, in ITALY in 45, it appears that results were NIL in 45 also. When the change took place on 1 Jan 44 the Germans started studying the traffic and after a while assumed that the code book had been changed, once more, as well as the recipher book or set of tables. They suspected that the recipher book or set of tables (WURMBUCH) was changed daily by means of use of a stencil (EINE SCHABLONE) which altered the order in which recipher groups were selected for reciphering code groups.

B. Description of Code and Recipher System.

I. The Code Book.

PW described No 5 Code of which he had seen a photostat copy as a four-figure book of 30,000 groups, in reality a set of three books each with groups ranging from 0000 to 9999. The code was issued in the form of an encode volume and a decode volume, each in three parts. The three parts of each volume were called:

the Ships List - containing all RN & (?) US Navy HQs (DIENSTSTELLEN).

the Main Code - code book proper.

the Geographical List - containing all geographical names.

Code groups from either of the a/m parts of the code were used in conjunction with indicators (ANKUENDIGUNGSGRUPPEN). These were listed at the beginning of the volume (encode and/or decode)

Indicators were: SL = "following group is to be taken from Ships List"
C = " " " " " " " " Main Code"
Geo = " " " " " " " " Geogr. List"

A number of four-figure groups were provided as variants for the clear indicators (SL or C or Geo). PW thought clear Geo was allotted 20 code groups. Spellers were used in Main Code with approx 10 variants each. The clear word SPELL was allotted 50 code groups. PW also thought that the code (volume containing three parts) included a "battle code" (GEFECHTSCODE) at the end of the book, but that this was never used by auxiliary vessels. Asked how many groups there were on each page of the code book, PW said he was not sure, but thought there were probably 50 to a page.

No (?) 6 Code - partially reconstructed by Mar 43 - was the same clear book, with a different arrangement of code groups. PW thought the last book the German Navy Cryptographers read, i.e. in use from end Apr or beg May 43 to end Dec 43, was No (?) 7.

PW quoted from memory the following Code groups out of either book (?) 6 or book (?) 7.

Shipping Index	= 9043
spell	= 2820
from FOCOS	= 9088
C in C Plymouth	= 6528
Geo List	= 1936
Shipping Index	= 3112

(N.B. All other groups in report are for example's sake.).

II. The recipher system.

The recipher book or set of tables (WURMBUCH) consisted of approx 100 pages, each page having 5 columns and 20 - 30 lines. The Germans had reconstructed this to the extent of knowing the following details of its use:

(a) at the front of the recipher book, or set of tables, there was a list of "starting point indicators" giving page and line on which reciphering begins, e.g. 8888 = page 30 line 9. These indicator groups were four - figure groups printed on a page and hatted. "Starting point" meant always the middle group, i.e. the third, on any given line.

(b) with the aid of a separate table - on the last page of the book, probably - these recipher indicators were camouflaged (reciphered once more = UEBER-SCHLUESSELT) so that the indicator which was signalled had to be broken before finding the group giving the "starting point". This table contained bigrams ranging from 00 to 99, and against these were placed the camouflage subtractors for any "unreciphered" indicator group. Thus: 8888 = page 30 line 9, is subtracted from 7818 and camouflaged to 9030 and this process is indicated by means of bigram 25. PW stated that clerks at OKM had told him that at the beginning of the war the recipher indicator was not camouflaged. Bigram 25 was signalled as part of the five-figure recipher and code indicator group in message, see III. below.

(c) recipher pages or tables were divided into pages (or tables) for reciphering addresses and signatures and pages (or tables) for reciphering text. The Germans thought that even pages (the pages on the left of the book) were used for reciphering addresses and signatures and marked them in red, (der ROTE WURM) and that uneven pages (on the right of the book) were used for reciphering text and marked them in green (der GRUENE WURM). This continued till Dec 43, after which date all recipher groups were taken from the same pages or tables, the latter changing daily. The reciphering of a message proceeded in this manner: assume uncamouflaged recipher indicator to read 8888, which means "starting point" is on page 30 line 9 (always middle - 3rd - group) and that the address is six groups long; the 3rd, 4th and 5th groups of line 9 and the 1st, 2nd and 3rd groups on line 10 of page 30 (even, red) would be used to recipher the encoded address. The first encoded group of the text would then be reciphered by means of the 4th group on line 10 of page 31 (uneven, green) and so on, and if the text was long, the 1st group, line 1 on page 33 would be used, etc. Signatures were NOT signalled. (Usually a message - in code - contained address only if retransmitted by WT sta, etc; i.e. in case of doubt as to who originator was. Otherwise there was NO address either. E.g. ((RED subtractor) SI (No) FROM FOCOS (GREEN subtractor) text).

(d) Recipher groups (4 - figures, were subtractor groups from which code groups (4 figures) were subtracted (non-carrying). The German cryptographers at OKM used the formula F = W - C i.e. marconigram group (FUNK GRUPPE) = recipher group (WURM) minus code group (CODEGRUPPE). E.g.

W	0000
C	1234
F	9876

(W - F will equal C).

III. Traffic and indicators.

Intercepted messages had the following lay out - PW quoted an example from memory (figure groups NOT real) - e.g.:

(see over)

MTA = to = 2 DAK = W = 2WWX = 25 1730B

25000 9030 .... etc

.... 9030 25000 25 1730B

where MTA (SCHIFF WT sta) is a land WT sta,
" 2DAK " " trawler
" W repeated
" 2WWX " " trawler
" 25 1730B " Date and TOO group
" 25000 stands for bigram 25 camouflageing the recipher indicator group (8888) to 9030 and 000 code book indicator (VERFAHRENSKENNGRUPPE; 100 variants provided).
" 9030 is camouflaged recipher indicator (8888).

C. Cryptography - Methods and Results.

I. Sorting of Traffic

Intercepted traffic brought to OKM SKL Chef MND III (after 1 May 44: 4 SKL III) was first sorted out according to code books (VERFAHREN) in a dept referred to by PW as the VERTEILUNG (i.e. TRAFFIC SORTING OFFICE). This was done by clerks instructed to do the sorting by looking for certain characteristics in the preamble of the message (Fu SPRUCHKOPF). The details concerning traffic in all types of known codes (reconstructed or under study) were supplied to traffic sorters by the registration or indexing personnel.

II. Breaking the Recipher - Methods Used.

The next stage was the research and/or work on breaking the recipher. (NOTE: Messages came to MUENCHEN BRAUN where only one type of code was being worked on, so that once GAs knew the traffic was in that code (AUXILIARY VESSELS CODE) work on breaking the recipher went straight ahead). At all periods P W was connected with OKM this work proceeded more or less on the same lines. PW is no cryptographer and can therefore not describe how the recipher was first broken, methods of approach etc. He can, however, describe the "drill" in some detail. There were six methods or ways in which the recipher book or tables could be broken (Mar 43 and earlier - Dec 43). These were:

(a) with the aid of two or more messages with the same indicators, say messages A and B both starting and ending with 25000 9030 (9030 25000). This constituted what the Germans called "eine SERIE". It amounted to working on two messages reciphered with subtractors taken from the same "starting point" in the book, during the same fortnight.

(b) with two or more messages with the same "suspected" recipher group (mit selbem VERDACHTSWURM).

(c) with two or more messages containing chance repeats (durch reine DOPPELVORKOMMEN) - this was done with the aid of HOLLERITH machines.

(d) through "rolling" (durch ROLLEN), a process necessitating the use of a device called the "ROLLMASCHINE" (see Appx "D" of report) whereby hypothetical marconigram groups were formed with the aid of known marconigram groups ("Bilden von kuenstlichen Fu-gruppen durch bekannte Fu-gruppen")

(e) through (breaking) deciphering of indicator groups (durch Entschluesselung der Einsatzgruppen) either (i) through a "chain of indicators" (eine SCHLUESSELKETTE) or (ii) through a "ring of indicators" (ein SCHLUESSELRING)

(f) by means of differencing (DIFFERENZIEREN).

III. Breaking the Recipher - Details.

(a) Messages with pairs of indicators

E.g. messages A and B:

A		B	
3 pen		gbxz	
(v) vpu		(v) mta	
1) 25000		1) 25000	
2) 9030		2) 9030	
3) 2560 — 1500 / 9040		3) 1728 — 1500 / 0882	(V)
4) 1735 — 4755 / 3020	ship and authorities in area	4) 9035 — 4755 / 5720	SCAPA WT
5) 8020 — 9995 / 1975		5) 6070 — 9995 / 3925	weather forecast
6)		6) 1718	till/until
7)		7)	
8)		8)	

By means of call-signs of originator and addressee a fitting (suitable) clear text was assumed for message A. The code groups corresponding to such clear text were looked up and written under the line in place marked ②, (drawn in black pencil), say 9040, 3020, 1975 etc, and then the "suspected" subtractor (VERDÄCHTS-WURM) group was calculated and written above the line in black pencil, in place marked (XG). (W=F+C). The "suspected" subtractor groups in the above example would have been 1500, 4755, 9995 etc. If, when applied to message B, these "suspected" subtractor groups (1500, 4755, 9995 etc) gave code groups, say 0882, 5720, 3925, which stood for clear text fitting that type of message, then the "suspected" subtractor group was "confirmed" (der Wurm wurde echt gemacht) and underlined in red and registered as a confirmed subtractor group (Echter Wurm). It could be used for the current fortnight. The Messages A and B were then said to form a "SERIE". If three messages were in a "SERIE", work would be easier, however this was not often the case. When, during the work of breaking the recipher (WURMZIEHEN) the point was reached where spellers were used, progress was slower, but headway could be made going from A to B and then from B to A, fitting in syllables or letters in one and confirming them in the other message. Time and date groups helped in the work. Time was encoded say 18 (group) and 00 (group). Cryptographers always tried 00 first.

This method was always tried first before going over to (b) or (c) etc, below. If messages were of the same length this was considered favourable and up to 70% of the text of telegrams could be read. The Germans estimated to intercept about six pairs of messages with the same indicators per day - thus getting six "SERIEN". Such occurences were all the more frequent the nearer the end of the 15 day period approached.

(b) Messages with the same "suspected" recipher (subtractor) group. (SERIEN mit selbem VERDÄCHTS/URM).

Example: addresses (call signs) of message:

from: (V) MTA = SCAPA WT

to : 2 GZB = G GZB = GBXZ = TANGO (trawler) with SI code name of 1230

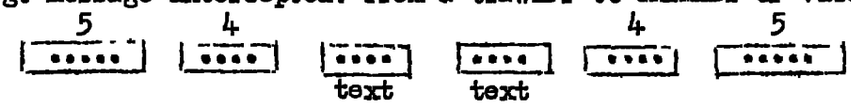
(NOTE: GBXZ is call sign of ship from the "INDICATIF d'APPELS" encoded to GGZB and reciphered to 2GZB).

E.g. contents of message:

1) 91345
2) 1250
3) 3020 — 2063 / 9043 — SI
4) 1590 — 2720 / 1230 — TANGO
5) 2535 — 8085 / 6550 — (V) FOCOS
6) ....

The CA assumed that group 3020 stood for clear SI and that this clear concept was encoded by means of code group 9043 (known). He then calculated the "suspected" subtractor (VERDACHTSWURM), i.e. 2063, and marked it with a red dot (in place marked ⊛) to show that it is a "suspected" subtractor.

This was done mostly for addresses (red subtractors). These "suspected" subtractors were then indexed (REGISTRIERT) and if another message with the same "suspected" subtractor was found it was placed next to the first one to be worked on. However, the second message had to show the same "suspected" subtractor group (say 2063) in either the same place in the message (in this case 3rd group) and the message was then referred to as an "identical key series" (eine SCHLUESSELGLEICHE SERIE), or in a place at intervals of 5 (number of columns in the recipher book) (PHASENGLEICH) i.e. 8th, 13th, 18th group, etc, in which case it was called "a biter series" (eine BISS-SERIE), AND also the subtractor had to be of the same colour (red or green). If the "suspected" subtractor, when applied to both messages, formed a "SERIE" and yielded clear text fitting these two messages, the subtractor was confirmed, underlined in red and registered. Approx 5 pairs of messages could be broken - up to 70% of text - every day. This was an average figure, PW said, results being always better towards the end of the 15 day period. Short messages yielded good results, because it was known in this case that the subtractor must be green (text only). E.g. message intercepted: from a trawler to GRIMSBY or vice versa:



Text is fitted in such as: sweep completed, or
request gate etc

or if from GRIMSBY
to trawler e.g.: gate arranged.

This saved a fair amount of time as fewer possibilities (place of clear text and subtractors) had to be tried out.

(c) With the aid of messages containing chance repeats (reine DOPPELVORKOMMEN)

E.g.

	A	B
1)	25705	35999
2)	1635	7984
3)	1590	1590
4)	9954	7638
5)	1718	
6)	1925	
7)	1777	
8)	8536	

With the aid of HOLLERITH machines pairs of - or more - messages were sought in which the same maroonigram group (Fu-GRUPPE) occurred in the same place, removed at an interval of 5, or multiples of 5, groups (PHASENGLEICH); in this instance 8th, 13th group, etc. PW said that in approx 50% of cases this was mere coincidence (ZUFALL) i.e.

	subtractor X	and	Z
code	Y		U
maroonigram group	1500		1500 ,

the percentage of coincidences (50%) being roughly the same for both red and green subtractors. However, all cases were tried out and if, say in the above example, clear text fitted in message A (3rd group, 1500), the same clear text was assumed to be in the 3rd group of message B as well. If the assumption proved to be correct, about 70% of the messages concerned could be read (Aug/Sep 43).

(d) Finding pairs of messages ("SERIEN") through "rolling" (durch ROLLEN).

This work was done with the assistance of the "ROLL" Gruppe (see para 3. C. I.c and Appendix "D" of report) and by using material supplied by the HOLLERITH machine (?) sub-sec. The various stages of the work are listed below:

(i) - with the aid of HOLLERITH machines a catalogue was drawn up, of all marconigram groups intercepted, listing groups in numerical order, from 0000 to 9999.

(ii) - the catalogue of intercepted marconigram groups listed traffic for a fortnight and separated - by means of markings - red from green subtractor-groups.

(iii) - high frequency known code-groups were then set on the machine (for "drill" see Appendix "D" of report).

(iv) - all known confirmed subtractor groups (bekannte echte WUERMER) were then taken out of the reconstructed recipher book (WURMMOGEN) and put through the machine in the hope of getting "artificial marconigram groups" (KUENSTLICHE FUNKGRUPPEN). These were looked for in the catalogue mentioned above and if found to occur in two messages in the same place, or at intervals of five, or multiples of five, the messages in which these "artificial marconigram groups" occurred were located and a pair ("SERIE") formed. The work was then handed over to cryptographers ("WURMZIEHER").

(v) - the cryptographer(s) then proceeded along these lines: E.g. messages A and N :-

A	N
.....	.....
1567	....
3026	3026 or in 8th, 13th, 18th groups, etc.
1738 (SI)	
....	
....	
etc	

(vi) - the code-group (e.g. 9043 = code for SI) was known. The cryptographer then tried to find out if the "artificial marconigram groups" 3026 found to occur in messages A and N were a reciphered version of the same code-group, or whether it was perhaps a coincidence. In the latter case the messages were separated, no pair ("SERIE") being formed. If, however, by fitting in a code group for relevant clear text, that code-group appeared to have been used - with recipher - in making up the "artificial marconigram groups" now found in these messages, then work proceeded on the two messages A and N.

(vii) - the messages were then placed side by side and the subtractor groups which had been used to recipher the known code groups in message A were applied to the same (or relative) marconigram groups ("artificial") in message N.

(viii) - PW stated that this work was done at the end of the 15 day period.

(ix) - results were mainly of historical interest.

(e) Finding pairs of messages ("SERIEN") by means of breaking or deciphering of indicator groups (durch Entschluesselung der EINSATZGRUPPEN (or) KENNGRUPPEN).

This could be done by attempting to break "a chain of indicators" (eine SCHLUESSELKETTE) or "a ring of indicators" (ein SCHLUESSELRING).

(i) "A chain of indicators".

A pair or more messages ("SERIEN") found by other methods (a - c) were required. E.g.

A	B
25000	51000
1527	5715
....	....
....	....

(NOTE: It did not matter if trigrams in five figure groups were the same or not, because they indicated type of code book and had many variants. 000 could be the same as 123, etc, in clear.).

Assumption: The messages A and B, being in the same "SERIE", have actually been reciphered by means of the same table and the reciphering proceeded from the same "starting point". Groups 1527 and 5715 are camouflaged (reciphered) "starting point" indicators, the four figure group with which reciphering was done being indicated by bigrams 25 and 51 respectively. (Cf para 6.B.II.b.). It was therefore assumed that the uncamouflaged "starting point" indicator in such a case was 0000 (die RELATIVE GRUPPE) therefore the camouflage or recipher groups against bigrams 25 and 51 (on last page of recipher book) would have been 1527 and 5715 respectively. (The German CAs referred to 0000 in this case as the RELATIV GRUPPE). These "assumed" recipher groups (die angenommenen WUERME) were then used as subtractors for all reciphered (camouflaged) indicators in messages with bigrams 25 and 51 which had been registered, and were outside pairs ("SERIEN"), for the 15 day period. (Recipher indicators (EINSATZGRUPPEN or KENNGRUPPEN) were registered in numerical order for easy reference). Thus:

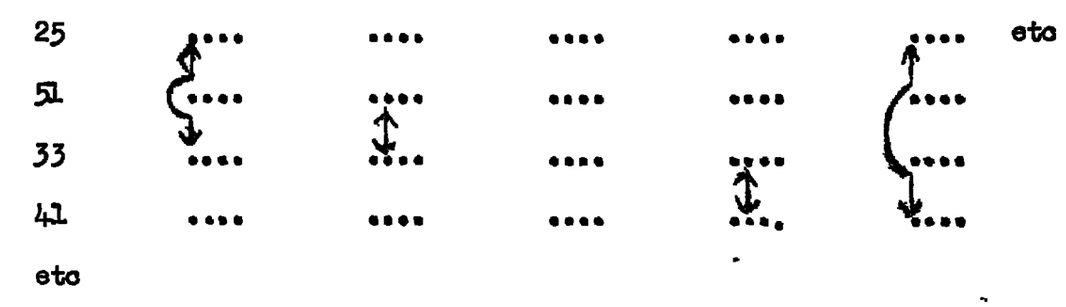
Messages with bigrams:				"X"	
	(AW)	1527	1527	1527	1527
	(F)	5090	6523	7956	8719
25		6537	5004	4671	3818
	(AW)	5715	5715	5715	5715
51	(F)	9876	1245	1144	6633
		6949	4570	4671	9182
				"Y"	

The common difference of 4671 was regarded as proof that the "starting point" indicator - uncamouflaged - was the same in the case of these two messages (X and Y). The complement of this difference (6439 = 0000 - 4671) was taken as the difference between the original recipher (camouflage) groups used to conceal the true "starting point" indicator. A new "SERIE" was thus formed, it being assumed and proved that, under the camouflage, messages X and Y were reciphered with the same subtractor (WURM). The pair of messages was then handed over to cryptographers, who carried on working as at - (a)--------above.

(ii) "A ring of indicators".

This was achieved when, by taking all messages with all bigram recipher camouflage indicators, the "chain of indicators" could be completed for traffic passed during the relevant fortnight. In such cases all messages could be linked together via their bigram recipher camouflage indicators. (Interrogator's Note: PW was not very knowledgeable or certain on this point).

E.g.:



Arrows show common differences between the two four-figure indicator-groups concerned.

PW stated that this method ("chain" and "ring of indicators") allowed the Germans to break into an additional 150 - 200 pairs of messages ("SERIEN"), but that these messages could only be read to the extent of 20 - 30% of text. The work was done at the end of the fortnight and took about 1 - 2 days. It was done by the extra-watches (PLUSWACHEN). This brought the total of 300 - 400 pairs of messages ("SERIEN") per fortnight - found by methods (a) to (d) above - to approx 500 - 600.

(f) Differencing (DIFFERENZIEREN).

PW described this method as "a variety of rolling" ("Eine Abart des Rollens"). Two kinds of differencing work were done at OKM:

(i) - differencing as an aid to recipher and code breaking; this was always done with the aid of the catalogue of differences (DIFFERENZENKATALOG).

(ii) - differencing done for the purpose of finding pairs of messages ("SERIEN") and "later series" (BISSE zu Serien); this type of work was begun in or after Dec 43 when the Fo (FRITZ OTTO) Group was specially formed for that purpose and carried on working on old material after 1 Jan 44 without results.

I. - Differencing as an aid to recipher and code breaking.

This was done when approx 20% of the Code book was known, not before. Two messages in a pair ("SERIE") were wanted. Each group in one message was "differenced" ("DIFFERENZIERT") through all groups in the other message and vice-versa. The smaller difference was always taken. Differencing was always done by hand - PW said no calculating machines were ever used at OKM - and all results were catalogued from 0000 to 4999.

E.g. 9043 - code for SI
6528 - " " C in C PLYMOUTH
3525 catalogued = SI - C in C PLYMOUTH.

Work proceeded on the principle of F1 - F2 = C2 - C1 when the same subtractor was used ("wenn der selbe Wurm Zugrunde liegt"), where F1 and F2 are marconigram groups (FUNKGRUPPEN) and C2 and C1 are code groups (CODEGRUPPEN), in messages 1 and 2. Cryptographers resorted to differencing when attempts to break the code in a pair of messages ("SERIE") showed no results. The group(s) in the messages where C's stopped, were differenced (smaller difference) same place in message or intervals of five), and the resulting four figure group was looked up in the catalogue of differences in an attempt to find clear groups which might fit in both messages. This was done separately for red and green subtractors.

E.g. Messages:

	A.	B.
11)	8765	1234
12)	....	....

The difference between the 11th groups in messages A and B i.e. 3579 was found in the catalogue to be for instance:

difference between:	WEATHER	and	SAIL
	SI		NOIC HOLYHEAD
	FROM		REPEATED (W)
	SPELL		GEO LIST
	etc		etc

If none of the above fitted in the text, differencing for groups 12, or 12 and 17, or 12 and 22, etc, were tried, and so on. PW stated that many CAs preferred to avoid differencing work, saying that "there were too many possibilities" to work on.

II - Differencing for purpose of finding pairs of messages ("SERIEN").

This type of work, which was done after the end of a current fortnight, necessitated knowledge of the code book to the extent of 50% - PW did not explain why Group Fo (FRITZ OTTO) persisted in carrying on working after 1 Jan 44, when both recipher and code changed.

Two messages which were NOT in pairs ("SERIEN") and were "routine messages", were picked out. "Routine messages" were recognised by means of their preamble (TUSHERUCHKOPF). PW quoted from memory names of stas signalling "routine messages":

FREETOWN	3 AFM (SCAPA)
SCAPA WEATHER	3 QLT = AIG 298 (HOLYHEAD)
AIG 31	COAC - HALIFAX = AIG 306 or 312
HATSTONE - RNAST	AIG 54
SHIPS TO ROSYTH (QZS) (gates)	

All groups in two messages of this type had to be differenced place for place and at intervals of five (STELLENGLEICH and PHASENGLEICH). This was hard work, PW said, and had to be done by hand. PW was of the opinion that with the HOLLERITH machines available to OKM this work would not have been practicable by mechanical means.

The formula on the basis of which this work was done was: F1 - F2 = D, where F1 and F2 are marconigram groups (FUNKGRUPPEN) and D is the difference between F1 and F2, whether large or small (F2 always subtracted from F1). From this: D + C1 = C2 where C1 and C2 are code groups in messages 1 and 2. Strips of paper were used, like the one illustrated below (X), on which were marked: messages, say A and B, i.e. all groups in B subtracted from their opposite numbers in A, the relationship of groups (STELLENGLEICH or PHASENGLEICH) and the differences.

E.g.:

(X)

A - B
PHASE
1 - 5
1) 2499
2) 1102
3) 8978
4) ....

Marconigram groups:

(F1)		(F2)
9043	-	7654 = 2499
0015	-	9913 = 1102
9091	-	1123 = 8978

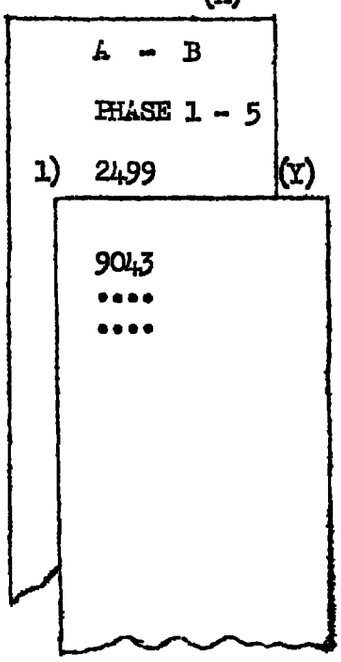
On another strip of paper ((Y) below) were written all known code groups which occured most frequently in message A. Assuming "routine message", was sent from AIG 31 and following groups were included:

(Y)

SI	= 9043 (real example)
bound	= 0033
sail	= 1234
PLYMOUTH	= 6533

Strip (Y) was then placed under strip (X) and groups added, in the same places or at intervals of five (STELLE FUER STELLE ODER PHASENGLEICH).

(X)



2499
9043
1432

It was then assumed that 1432 was the corresponding code group in message B, under recipher. Code group 1432 was looked up in the reconstructed Code book and if the clear word or syllable or text fitted message B, it was assumed that it was "good" and the next group was tried. PW illustrated this as follows. Assuming 1432 in message B (Y) FREETOWN = spell and the next group was tried and - spellers being expected - this group was either CA or MO. As a fair number of Spanish and Portugese ships were known to call at FREETOWN the spellers CA or MO could be assumed to stand for the first syllable of CABO or MONTE respectively. If the next group or two fitted the message, the full name of the ship(s) could be found with the aid of GROENER's Handbook of World Mercantile Fleets (TASCHENBUCH DER WELTHANDELSFLOTTEN). (Note: these mercantile ships lists etc. were useful only in case of neutral ships being mentioned in messages). If groups thus found fitted the messages, the subtractors (F - C = W) were registered and also tried out by "rolling" (Cf (d) above).

PW stated that the main aim of this method was to find new code groups. Most successes were achieved with FREETOWN traffic. Being in possession of 50% of code groups (reconstructed) the Cryptographers could get up to 70% by working according to this method.

IV) Registration of Code groups.

This was done by a team of three men referred to as code-interpreters (CODEDEUTER). All decoded material went to them and code groups were entered on cards, with indices of frequency etc. Code groups were classified as:

(a) Genuine code groups (ECHTE CODE GRUPPEN), marked with two crosses and underlined in red,

e.g. Sp $\frac{x}{x}$

(b) Half-genuine code groups (HALBECHTE CODE GRUPPEN), marked only with one cross.

(c) Assumed code groups (UNECHTE CODEGRUPPEN) - no marks.

A code group was considered to be genuine if it fitted in approx 100 places, half-genuine if it fitted in approx 50 places and an assumed one if it occured in approx 10-20 places.

7. WORK AT Fu REFERAT (FRANKFURT) AND OTHER SUB-UNITS

A. The Frankfurt System (VERFAHREN FRANKFURT).

This was the cover name for an RN code used by ships other than auxiliary vessels. PW thought it was a high grade code used by Flag Officers as well. It was read till end Feb 43. After that date NO results were obtained as far as PW knew.

B. RN and US Navy Tactical Codes.

I. General

PW stated that characteristic of most of these codes was the fact that they were all letter-codes and that only certain letters of the alphabet were signalled. Some codes were read at Intercept and DF HQs and/or Stas only, some were read at the OKM as well - see below.

PW remembered details of the following codes:

LOXO (3-letter code) and the COFOX (4-letter code) read throughout the war till (?) 44. STATION 31 at SOUTHEND transmitted traffic in these codes; work was done in Fq Group.

MEDOX (? 3-letter code), used in the MEDITERRANEAN, was read in '44.

NYKO (4-letter code) and the SYKO (4-letter code) were read till Mar 43, when they went out of use.

TRAXO and the ECCO (? letter codes) were read at OKM in (?) Fq Group; they were known as Invasion Codes (LANDUNGS CODE).

US Navy ? 4-letter codes AQUA, BIKE AND AMID were in operation after 6 Jun 44 and occasionally read at OKM, perhaps by Fq Group.

II. Details of LOXO and COFOX Codes.

The LOXO was worked upon at MP Abt FLANDERN at BRUGES and also at the OKM in the Fq Group where traffic from stas other than 31 SOUTHEND was available. Work in the Fq Group was under the direction of Dr. THOMA (see para 10 PERSONALITIES in Report). Results of cryptographic work at BRUGES were sent to the OKM in BERLIN for evaluation and completion. No captured tables or docs referring to LOXO were available, but it was broken successfully and read all the time. The system or the tables - PW was not sure which - changed in Oct/Nov 44, but traffic continued to be read. The LOXO was used for encoding traffic dealing with gates control in the THAMES Estuary by STA 31 at SOUTHEND, also by GRIMSBY and patrol vessels. The Germans found out that they could always break into the SOUTHEND traffic and every effort was made to take it. Station 31 being rather weak, when MP Abt FLANDERN moved from BRUGES to BRUSSELS in Jan 44 they set up a "directional antenna" (eine RICHTANTENNE) of 1000 m length trained on the exact bearing of SOUTHEND. The code was signalled in 3 letters; included among those used were: F, H, J, K, M, P, Q, S, T, U, X, Z. The Code was reciphered, the recipher changing daily.

The COFOX was on the same lines as the system outlined above. However, it was not used so frequently. It was also read at BRUGES. The Code was operated by the same type of ships and perhaps on inter-convoy traffic.

8. U-BOAT DF SERVICE (see also para 3 C.II a and Appendix "E" of report).

One of the tasks of MP Abt FLANDERN at BRUGES was the training and equipping of Intercept and DF operators for the German submarine service. Operators were required to speak English well and reach a good standard in RT interception and DF operation. PW stated that he knew of six operators who had sailed on board U-boats, but could only recall the name of one, a PO(WT) (Funk Maat) GROSSMANN, to whom he had spoken, and who claimed to have helped in the sinking of a British Cruiser in Mar/Apr 44. The German Navy Intercept Service had decided - after 43 - to attempt to place convoy escorts and meeting points at sea by means of RT intercept and DF methods on board U-boats. PW stated that until end Apr 43 code breaking results could be given to U-boats. After end Apr 43, when cryptographic results were still obtained, but with greater difficulty, it was decided to utilize these for strategic purposes mainly and rely - if possible - on U-boat DF for locating targets.

The operator sailed as part of the crew and was equipped with a TELEFUNKEN-EP2 special DF set (SPEZIALPEILER). (For details of EP2 and planned new equipment, see Appendix "E" of report). When the U-boat surfaced - desirable at times when convoy and escorts were on the air - the operator would listen in and get the bearing. The reading had to be reported to the Captain at once. PW thinks that one bearing was considered sufficient to give rough location of escorts and/or convoy because: (i) if heard on the air ships could be at a maximum distance of 100 miles (RT range), (ii) Allied convoys stretched over some distance - between leading and last ship - and (iii) what was really wanted was the bearing for setting a course in that direction. PW however confessed that possibly the Germans oversimplified the problem and overlooked such factors as a convoy changing its course after netting calls, or traffic being passed at a time when a U-boat dared not surface. Asked if DF was ever attempted from more than one U-boat and results communicated by WT to get a "cut", PW replied he did not think so, as "NO U-boat would dare to signal with enemy ships around".

Operators were instructed to listen-in to netting calls on the frequency 2410 Kcs (wavelength 124.5 m). (See also Appendix "C" para C.).

9. WORK AT "B" GRUPPEN NERVI AND SAN REMO. (PW worked in these units as a WT mechanic from Dec 44)

Work in the "B" Gruppen consisted in watching traffic in WT and RT, and such code and cipher work as was done was carried out with the help of material provided by OKM or an MPHS (in the case of NERVI and SAN REMO by MPHS KARERSEE).

"B" Gruppe NERVI watched the "Speedboats - frequency' (SCHNELL-BOOTSWELLE) of 2150 kcs. This frequency was watched both from the land sta (at the group) and from on board Italian and German Navy Units sailing in the LIGURIAN SEA e.g. (?) Italian T34s (destroyers or torpedo boats), LANCIA barques for amn tpt. Two operators (one for WT and one for RT) sailed on each ship or convoy and reported to Captain i/c ship(s) any contents of messages intercepted from Allied ships trying to attack them. Traffic taken at NERVI by operators stationed on land was sent to MPHS KARERSEE.

"B" Gruppe SAN REMO watched mostly RT traffic originated by the French. The frequency of French patrol boat traffic was 2716 Kcs and traffic was in a code made up of cover names (on TARNTAFEL lines) with names of colours for clear figures. The code changed at the end of Mar 45. PW stated that traffic was partly read, mainly because the French were so careless.

10. PERSONALITIES.

(Ranks are given in German with English equivalents in brackets, where applicable.)

Kpt-zur-See (Captain) BONATZ	Head of Chef MND III (later 4 SKL III) till beg Dec 43. Rumoured to have been replaced by KUPFER below because he failed to make arrangements for security of docs etc which were all destroyed in a bombing raid on night of 22/23 Nov 43.

~~TOP SECRET~~

CSDIC/CMF/Y 37

Kapitaen (Comdr) BUDDE	I/c Evaluation (Chef der AUSWERTUNG) in Chef MND III, later 4 SKL III. Was there at beg 44.
Oberregierungsrat Dr FRANKE	Head of Generalreferat ? dealing with US Navy traffic.
Funk Maat (PO(WT)) GROSSMANN	U-Boat DF operator.
Kpt-zur-See (Captain) KUPFER	Replaced BONATZ above at beg Dec 43 as head of Chef MND III (later 4 SKL III).
Faehnrich (Cadet) later Leutnant (Sub-Lieut) LUSEBRINK	I/c watch (WACHLEITER) in Fu Referat (MUENCHEN BRAUN) and did good work on Auxiliary Vessels Code (FREETOWN traffic).
Regierungsrat Dr SCHEUERLE	Took over Fm Referat when formed, in Dec 43, by amalgamation of STTETIN, HAMBURG, and BREMEN Secs.
Amtsrat SCHULZE	Worked under Generalreferat "F" on SWEDISH Naval traffic in Jul 44. An ex WT operator, O.R..
Amtsrat SCHWABE	Head (Referatsleiter) of Fu Referat (FRANKFURT).
Leutnant (Sub-Lieut) Dr STAUDT Arnim	Till 1 May 44 "Adjutant" to STUMMEL. Should know of Asdic defence measures planned by Chef MND IV (later 4 SKL IV). Has lived in the ARGENTINE, speaks Spanish.
Admiral (Adml) STUMMEL	Head of Chef MND (I-IV) in 43 - May 44. Interested himself mainly in Asdic defence.
Regierungsrat Dr THOMA	Head of Fq Group, dealing mainly with LOKO. Ex MP Abt-FLANDERN (BRUGES).
Oberregierungsrat TRANOW	Head of Generalreferat "F" (Gt.BRITAIN & RUSSIA). Peace time cryptographer, perhaps ex-MPHS LANGENARGEN (Lake CONSTANCE).

C.S.D.I.C.,
C.M.F.
3 Jul '45

(W.S. VALENTINE),
Lt-Col,
Comdt. CSDIC., CMF.

REF ID:A65385

Appendix "A"

~~TOP SECRET~~

CSDIC/CMF/Y 37

PATTERN OF GERMAN NAVY INTERCEPT WT FORM.
(FUNKSPRUCH BLOCK FORMULAR).

Intercept Sta B-STELLE: Range (Area) BEREICH: | No. Date: DATUM: Frequency: FREQUENZ: Time of Taking. AUFN. UHRZEIT: From: VON To: AN: DF: PEILUNG: in degrees.	Preamble FUSPRUCH KOPF No. of GROUPS GRUPPEN No.	Space used for Registration etc. 23/9030 TOO Group UHRZEIT GRUPPE.

1	25000		16	
2	9030			
3	2560	1503 9043	SI	
4				
5				
15			30	

~~TOP SECRET~~

OSDIC/CMF/Y 37.

Appendix "B".

PATTERN OF GERMAN NAVY INTERCEPT LOG BOOK FORM.
("B" STELLEN TAGEBUCH FORMULAR)

Intercept Sta.	Zone:	Operator.	Date:	No:
B-STELLE:	BEREICH:	HORRER:	DATUM:	

Time	Frequency Kos WELLE	From.	To.	Contents and Remarks
UHRZEIT.	KHz	VON	AN	INHALT UND BEMERKUNGEN:

Appendix "C" (Cf para 3.C.II. of report)

DETAILS OF WT STAS COVERED BY THE GERMAN NAVY INTERCEPT SERVICE. CALL SIGNS & FREQUENCIES MEMORISED BY PW.

A. WT STAS COVERED BY GERMAN NAVY INTERCEPT SERVICE (1943-1945).

UNITED KINGDOM:

WHITEHALL
FLEETHORPES
SCAPA
ROSYTH
AULTBEA
GRIMSBY
GREAT YARMOUTH
SHEERNESS
SOUTHEND
DOVER
BRIGHTLINGSEA
RAMSGATE
NORTH FORELAND RADIO
PORT PATRICK RADIO
PORTSMOUTH
DEVONPORT
PLYMOUTH
FALMOUTH
HOLYHEAD
LIVERPOOL
GREENOCK
LONDONDERRY
INCHKEITH
MAY ISLAND

BRITISH EMPIRE:

HALIFAX
ST. JOHNS
VANCOUVER
SUVA (Fiji)
FALKLAND ISLANDS
TRINCOMALEE (Ceylon)
CALCUTTA
BOMBAY
ADEN
ALEXANDRIA
BASRA
NICOSIA (Cyprus)
GIBRALTAR
RINELLA (Malta)
FREETOWN
ST. HELENA
WALVIS BAY
SIMONSTOWN
DARESSALAM
SLANG KOP Pt.
TAKORADI
ESQUIMALT
AWARUA
BELCONNEN
FLINDERS Isld.
KILINDINI

U.S.A. & DEPENDENCIES:

ANNAPOLIS
MIAMI
HONOLULU
SUMMIT BALBOA
COCO SOLO
GUANTANAMO
KODIAK
SITKA

BASES IN OCCUPIED TERRITORIES INCL. INDIGENOUS STAS.

BEIRUT
ALGIERS
BISERTA
TUNIS
RABAT
CASABLANCA
PORT LYAUTEY
DIEGO SUAREZ (Madagascar)
AZORES
BASTIA
PALERMO
NAPLES
LEGHORN
MARSEILLES
NICE/VILLEFRANCHE
CANNES
CHERBOURG
LE HAVRE
MORLAIX
RENNES
PARIS
ANTWERP
BRUSSELS
BRUGES
REYKJAVYK
GREEN HARBOUR (Spitzbergen)
GAMMATRON (Greenland)

RUSSIA:

MURMANSK
ARCHANGEL

BRAZIL:

RIO DE JANEIRO
RECIFE PERNAMBUCO

Appendix "C" cont.

B. CALL SIGNS.

I. NAVAL GENERAL CALL SIGNS.

PERIOD:	STATION:	CALL SIGNS: WT	RT
1943/44	WHITEHALL	GYA	
	CLEETHORPES	GYE GYB	
	GRIMSBY	MFC	
	SCAPA WT	MTA	BULL TANNER/SCAPA
	DOVER	MTU	DOVER
	LIVERPOOL	MAD	MAD
	LIVERPOOL SHIP		RABBLE, SILEX, GALEX, LIFEBAG
	INCHKEITH		ISAAC
	MAY ISLAND		MOSES
	DEVONPORT	MTN	
	SHEERNESS		BULL SAFETY/SHEERNESS
	SOUTHEND		31, 36, 47, 48
	FREETOWN	VPU	
	BELCONNEN	VHP	
	GIBRALTAR	GYX	
	HALIFAX	CFH	
	ANNAPOLIS	NAA	
	SUMMIT/BALBOA	NBA	
	LOA LOUA LAI/HONOLULU	NPM	
	CHERBOURG	NJS	NJS
	PARIS	NJI	NJI
	MARSEILLES	FUM	FUM
	LEGHORN	MJD	MJD

II. NAVAL BASES AND AUTHORITIES.

1943/44
- SHIPS GRIMSBY AREA - 3 PIC
- SHIPS AND AUTHORITIES IN AREA P3 FREETOWN - 3 PEU

III. USED BY: ?

1944
- CODE NAMES: (RUFFLEMEN) — figure - letter - figure
- " — 6 - letter - letter - letter
- " — 7 - letter - letter - letter

IV. SHIPS AT SEA:

1943/44 { CODE NAMES: (RUFNAMEN) from AB to AZ

V. INTERALLIED CODE NAMES (INTERALLIERTE RUFNAMEN):

1943/44 letter - figure - letter - figure - letter.

VI. TRAWLER CODE NAMES AS PER "INDICATIF D'APPELS":

1943/44 2 - letter - letter - letter.

VII. DELIVERY GROUPS (VERTEILER GRUPPEN):

UD = also intended for.

1943/44 QG = pass to.

HJ = Admy. (Admiralty)

VIII. DELIVERY - ADDRESSES (VERTEILER ADRESSEN):

1943/44 Letter - letter - letter.

C. WAVELENGTHS AND FREQUENCIES - (1943-45).

(NOTE: PW quoted either wavelengths in m. and/or frequencies in MCs. These have been converted into Kcs and are shown in col. 3.)

1 WAVELENGTH m	2 FREQ. MC	3 FREQ. Kcs	4 USED by STAS AND IN ZONES:
35	8.2	8200	MTBs (KLEINKAMPFVERBANDE) in the ENGLISH CHANNEL.
	8.4	8400	
	8.5	8500	
93		3225.8	N.FRANCE, after the invasion.
97		3092.8	
	2.7	2700	STAS: NJS & NJI in N.FRANCE.
110	2.716	2716	FUM-MARSEILLES.
113		2654.9	INVASION AREA (N.FRANCE).
120	2.5	2500	C in C PORTSMOUTH, PLYMOUTH.
122.4		2451.8	
124.5	2.41	2410	CONVOY ESCORT FREQ (GELEITZUGSWELLE).
	2.45	2450	PATROLS S.FRANCE COAST- (BRETON, P1 & P2).
	2.24	2240	UNKNOWN (TARTAR, NORTON, CROSSWISE).
137	2.26	2260	SCAPA, INCHKEITH, MAY ISLAND (FOCOS).
137.6		2107.7	LIVERPOOL M.D to "RABBLE" (C in C WESTERN APPROACHES).
	2.15	2150	SPEEDBOATS in MEDITERRANEAN (Gulf of GENOA).
147.5	2.04	2040	RAMSGATE to "SHEPHERD".

1 WAVELENGTH m	2 FREQ. MC	3 FREQ. Kcs	4 USED by STAS AND IN ZONES:
	2.068	2068	SOUTHEND 31 to THAMES Control ships.
155.4		1995.5	SHEERNESS.
168.5	1.78	1780	CiC NORE, GRIMSBY, GREAT YARMOUTH, NORTH FORELAND, PORT PATRICK RADIO.
170		1765	DOVER.
172 176 188		1744.5 1704.6 1638.4	Alternative frequencies (AUSWEICHWELLEN).

Appendix "D"

(of para 6.C.III.d. iv of report)

A. Description of ROLLMASCHINE. (FIG 1 on Appendix)

PW compared it to an abacus and gave the following details of its construction and handling. The machine is composed of a metal-sheet outer casing of which the top side is illustrated in FIG 1. (area a b c d). The top side of the machine has a cover which can be opened (area e f g h) and part of which (area e f i j) is covered with glass allowing operator to see the first "rollers" on each of the four axles (axles with rollers marked k l m n). The remaining part of the top cover (e f g h) i.e. area i j g h, has four open channels through which operator can see the rollers turn. On the "window" (area e f i j) and the left hand side of cover (a e c g) strips are provided on which the subtractor group set on the machine's top rollers and the code groups, can be marked before operating. The four axles (k l m n) have usually 10 (sometimes 15) "rollers" mounted on them. The machine is built in such manner that when the top cover (e f g h) is opened the "rollers" can move independently on the axles on which they are mounted. When the top cover is closed, the axles can be moved and all "rollers" on the one axle move with the axle, but not independently. The axles are not coupled, they have to be moved individually. A support is provided with the machine allowing operators to place it on their desks at an angle of approx 45° from the horizontal.

B. The "Rollers" (Cross-section illustrated in Fig 2 of Appendix).

The "Rollers" are made of wood or metal, diameter approx 1 inch and are marked from 0 to 9 in an anticlock-wise direction. When the machine is operated the axles on which the "rollers" are mounted are turned in a clock-wise direction so that 1 follows 0, 2 follows 1 etc.

C. "Drill" for setting the machine. Suppose the groups (high frequency known code groups) 9043, 2820, 6528 etc have to be put through the machine. They are written out on the strip at the side of the machine (area a e c g) starting from a line corresponding with the second row of "rollers". The top cover of the machine is opened, allowing "rollers" to move independently on their axles and the "rollers" are set at: (see Fig 1)

0000 on the top row
1067 " " 2nd " } 1067, 8280 and 4582 etc being the groups
8280 " " 3rd " } of complements of digits (das SPIEGELBILD)
4582 " " 4th " } which make up the code groups.
etc

The group 0000 is the basic setting (GRUNDEINSTELLUNG) for the subtractor trials and is always taken - arbitrarily - for the sake of convenience. PW stated one could set the machine at 1111 (on the top row of "rollers) or any figures, but one would have to carry on completing the cycle in any case (see D below).

D. "Rolling" - "drill". When the machine is set, all registered confirmed subtractor groups (found in the reconstructed recipher book - WURMBOGEN) are turned on the top row of "rollers", in turn, and the resulting "artificial marconigram groups" are compared with the catalogue of intercepted marconigram groups. If any "artificial" groups are found to exist in the catalogue and in the two messages, these are made into a pair ("SERIE"). In FIG 1 complement digits of code groups are set with assumed subtractor 0000. In FIG 3 confirmed subtractor 1257 has been set by "rolling" and "artificial" groups 2214, 9437 and 5739 obtained.

E. PW stated that this kind of work could ne done by hand also, but that it would take much longer. Therefore, instead of taking frequent code groups 9043 2820 6528 - suspected to be at the basis of some marconigram groups in traffic - and trying to subtract them from all confirmed, registered subtractor groups

known to the cryptographers, such as:

subtractor group (W)	1257	1257	1257	etc
code group (C)	9043	2820	6528	
marconigram group (F)	2214	9437	5739	

the complement values of code group digits are set on the "rollers", assuming that on the top row code group 0000 is set as a starting point, and subtractor 1257 for instance, and others, are added: E.g.

subtractor group (W):	1257
code group (C):	0000
marconigram group (F):	1257

subtractor groups (W):	1257	1257	1257
code groups (C):	1067	8280	4582
marconigram groups (F)	2214	9437	5739

The machine has the advantage of allowing several code groups to be treated at the same time.

F. "Rolling" is done separately for red subtractors applied to addresses - code-groups and green subtractors applied to text-code-groups.

~~TOP SECRET~~

CSDIC/CMF/Y 37

Appendix "D"

Fig 1

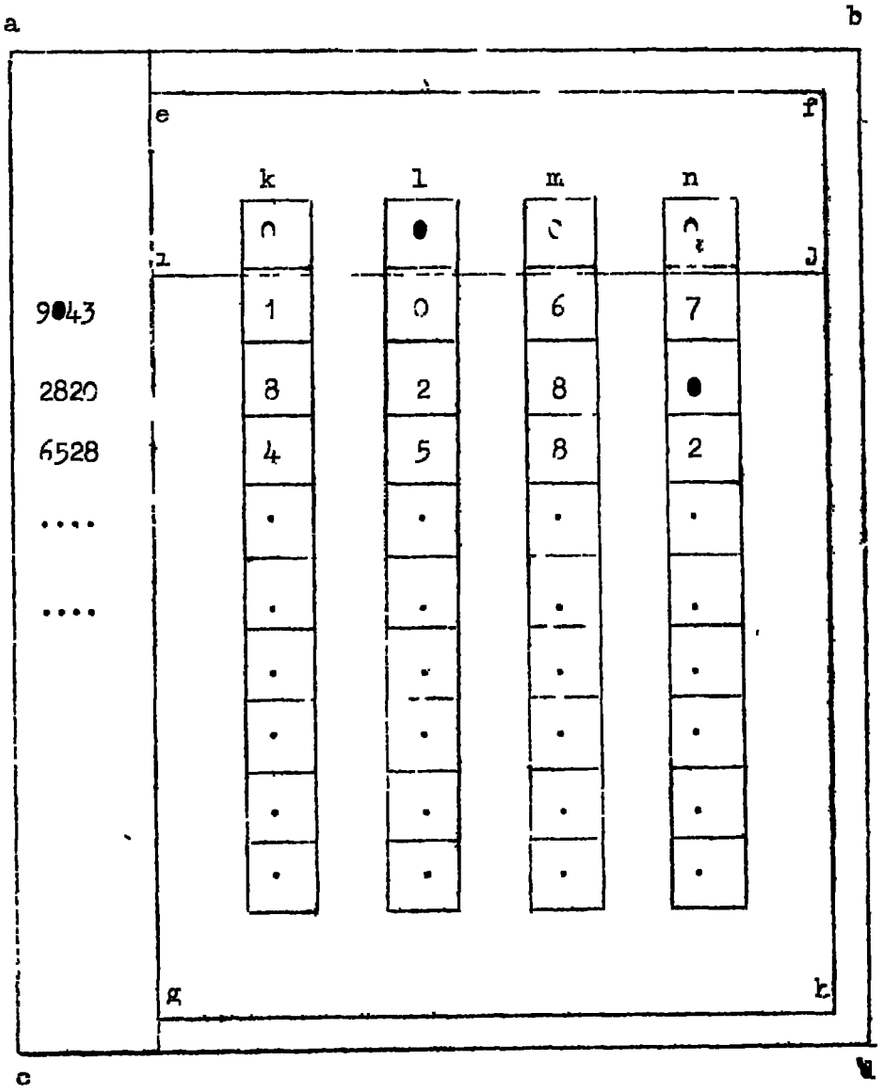


Fig 2

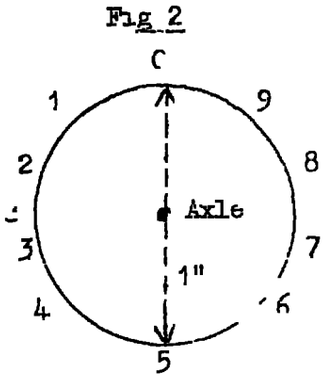
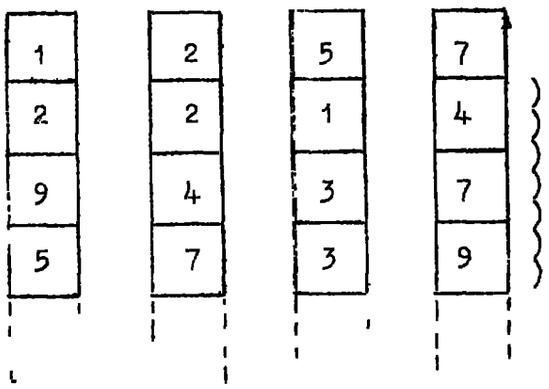


Fig 3



"artificial marconigram groups" (KUENSTLICHE FUNKGRUPPEN).

~~TOP SECRET~~

CSDIC/CMF/Y 37

Appendix "E" (of para 8 of report)

PW TEMP's DESCRIPTION OF U-BOAT SPECIAL DF APPARATUS & FU-MAAT GROSSMANN'S EXPLOITS.

U - Boot Spezialpeiler :

Als U-Boot Spezialpeiler wurde zunaechst der von Telefunken gebaute "EP 2" mit Peilrahmen und Hilfsantenne benutzt. Der EP 2 ist ein gewoehnlicher 4-Roehren Ueberlagerungsempfaenger fuer Batteriebetrieb fuer Grenz und Langwellen. Die Deutschen beabsichtigten spaeter einen von NVK (NACHRICHTEN VERSUCHS KOMMANDO) entwickelten "SICHTPEILER" zu benutzen. Der Sichtpeiler macht die Peilung auf einem BRAUNSCHEN ROHR sichtbar, so dass man ohne Ueberlagerung peilen kann. Das bedeutet dass man bei der Peilung von Fonie-Verkehr diesen Verkehr gleichzeitig abnehmen kann.

GROSSMANN hat nach seiner eigenen Schilderung bei seinem U-Boots Einsatz Fonie-Verkehr zwischen zwei britischen Einheiten festgestellt und diese eingepeilt. Auf die Peilung hin soll der Angriff auf einen britischen Kreuzer gefahren worden sein. Durch Ueberwachung des Fonie-Verkehrs nach dem Ungluecck und waehrend der Rettungsaktion will er die Versenkung des Kreuzers festgestellt haben.

TRANSLATION:

At first the TELEFUNKEN EP2 - with DF frame and auxiliary aerial - was used as a U-boat special DF set. The EP2 is an ordinary four-valve-heterodyne receiver, working on batteries, for medium and long wave bands (? 100 - ? 2000 m). The Germans intended to use later on a "vision" DF set ("SICHTPEILER) developed by the German Navy Sigs Experimental Command (Nachrichten Versuchs Kommando = NVK). The "vision" DF set permits the operator to get the beam on a cathode ray tube (BRAUNSCHE ROHR), so that DFing is possible without a superimposed wave. This means that when DFing RT traffic, the latter can be taken down simultaneously.

According to his own description while sailing on board an U-boat, GROSSMANN intercepted and DFed RT traffic between two British Naval Units. As a result of DFing an attack was made on a British Cruiser. He stated that he confirmed the sinking as a result of listening in to RT traffic after the catastrophy and during the salvaging operation.

~~TOP SECRET~~

CSDIC/CMF/Y

DISTRIBUTION

	Copy No.
AC of S G-2, AFHQ	1
COIS, MED	2 - 3
CIO HQ MAAF	4 - 5
G-2 (Sigs "I") AFHQ	6 - 8
S.I.S.	9
G-2 (P/W) AFHQ	10
GSI (s), 15 Army Group	11
MI 8, War Office	12 - 14
MI 19, War Office	15
File	16 - 18